In the Real-World Game of Cybersecurity

The Best Defense Is a Good Offense

BY S.A. SWANSON

The past year has generated some big headlines about data breaches—all with large companies on the losing end. But that doesn't mean smaller firms have escaped hackers' attention. The number of attacks reported by midsize companies (those with revenue of $100 million to $1 billion) increased 64 percent from 2013 to 2014, according to a survey PwC conducted with *CIO* and *CSO* magazines. For midsize U.S. organizations, the estimated average financial losses for detected incidents totaled $1.8 million per company.

"When I talk with senior people in government, they say they're more worried about the small and midsize companies, because the big guys are spending more money on cybersecurity," says David Burg, PwC's global and U.S. advisory cybersecurity leader. Attackers will want to spend time where they're more likely to have a higher rate of return, he says.

With relatively small staffs managing large sums of money, middle-market private equity firms easily fall into that category. "There are very attractive targets, like limited partners, who might be ultrahigh net worth individuals. (Cybercriminals) may want to go after that person or their family office to make fraudulent financial transactions," says Dave Dalva, vice president of security science for digital risk management firm Stroz Friedberg. "It's a dichotomy, in the sense that you have a smaller company with high-impact information. But they often have relatively immature security programs."

To defend against security risks, firms need to focus on the interconnected systems that pervade business interactions. That flow of information creates a cybersecurity ecosystem that encompasses not just the private equity firm, but also how it's linked to portfolio companies, service providers and even social media. Says Burg: "The reality is, every single business operates by managing information and data, and you have to think about where that data travels to really understand the ecosystem implications."

CRITICAL DATA: IDENTIFYING 'WHAT' AND 'WHERE'

To create a secure ecosystem, companies must address two fundamental questions: What information is most critical, and where does it reside? Cybersecurity experts have plenty of stories to demonstrate how often those questions are overlooked.

"I saw a situation where someone on the distribution list for the firm's deal strategy forwarded the email to an employee who didn't need that information," Dalva says. "And some of the key people in the firm were then a little concerned that the deal strategy, which is probably the most sensitive strategic document in the firm, is being sent around with very limited controls." At many firms, Dalva has seen a lack of understanding about what qualifies as sensitive information and who should access it. Employers should clarify that as part of their security policy and ensure all employees know about it, he says.

Firms also need to think broadly about what represents sensitive information in their ecosystem. "This is where a lot of private equity firms get tripped up, because folks tend to think about risk related to credit card or social security data," says Jim Ambrosini, a managing director with CohnReznick Advisory Group, where he leads the firm's cybersecurity and technology consulting practice. "There is an incorrect belief that if we don't have this type of data, we are probably less likely to be targeted and attacked."

Cybersecurity programs often aren't aligned with industry risks because firms treat cybersecurity as an IT issue. That's the wrong approach, Ambrosini says. "Cybersecurity is not an IT thing," he adds. "It's a business risk decision, and it requires a business strategy to deal with it." The CFO and other managing partners are in the best position to identify what information is most valuable, he says, and to ask the IT team what's being done to protect that data.

"WHEN I TALK WITH SENIOR PEOPLE IN GOVERNMENT, THEY SAY THEY'RE MORE WORRIED ABOUT THE SMALL AND MIDSIZE COMPANIES, BECAUSE THE BIG GUYS ARE SPENDING MORE MONEY ON CYBERSECURITY."

David Burg
Global and U.S. Advisory Cybersecurity Leader, PwC

Often, firms aren't fully aware of where their critical data resides. At PwC, Burg's team has seen this happen repeatedly with clients. "We'll find companies that have a new piece of IT infrastructure, and for the sake of performance testing, real data is put in there, and it may not be adequately protected," Burg says.

When it comes to controlling the location of sensitive data, the ubiquity of cloud computing can pose significant problems. "It's very cheap and easy to put data into the cloud," says Jerry Pender, who worked at the FBI for almost 13 years, including three years as chief information officer. "Any employee with $100 and a credit card can put gigabytes of data into a cloud service. And it can be very difficult to keep track of that."

To minimize the risk of employees going rogue, Pender suggests educating them about what information is most sensitive, what they're allowed to do with it, and the potential consequences of ignoring company policies. "If people aren't aware of what's important, they're going to make mistakes," says Pender, who now focuses on information technology and cybersecurity as managing director and operating partner at Z Capital Partners.

When tracking the flow of critical data, firms also need to carefully assess their vendors' access, which can represent a security weak spot. That was the case in Target's high-profile data breach—hackers entered the system after infecting the retailer's HVAC vendor. Most private equity firms probably haven't protected themselves against the vulnerabilities that could emerge if vendors are hacked, Ambrosini says. "Begin with some good questions. Any time a vendor is accessing systems and data, someone should be asking: Who is accessing it, what do they have access to, what do they need it for, who is controlling it, and how are vendors protecting that data?"

LACK OF CYBERDILIGENCE

When middle-market private equity firms conduct due diligence for potential investments, cyberrisk usually isn't a consideration. "They're looking at financial information, but they're not looking at it from the standpoint of enterprise risk," Ambrosini says. That's shortsighted, because a breach at a portfolio company can create both financial and reputational damage for the firm.

Dalva of Stroz Friedberg has developed an assessment of cybersecurity risk at potential portfolio companies—he says large PE firms have used the service, but not smaller ones. "I like to call it cyberdiligence," he says, noting the process involves speaking with the principals and technical staff of the company, and directly observing the company's infrastructure. Dalva's team recently conducted cyberdiligence for a large PE firm and found a couple of vulnerabilities at one portfolio company. "The PE firm is making sure the company addresses that as a condition for investment," Dalva says.

Israel Martinez, president and CEO of cybersecurity firm Axon Global, says he's seen data that suggest at least 20 percent of the companies being acquired have already had their intellectual property stolen by hackers. Before investing in a company, he recommends hiring a firm to research whether that company has already been compromised. "I would say 80 percent of (private equity) decision-makers are not thinking about it," he says. "But even when they are made aware of it, they're under the false belief that insurance would cover them later if there was an issue where there was nondisclosure about a breach."

DON'T TAKE THE BAIT

Social media creates security challenges too. That's because the information posted on LinkedIn, Facebook, Twitter and elsewhere can help hackers create effective spear-phishing campaigns. Spear-phishing represents the most common method of targeted cyberattacks and uses carefully crafted emails that trick employees into clicking on links or attachments that infect their computers.

By gleaning personal details about their targets, hackers can boost the success rate for their social engineering. "Let's say I'm on Facebook and I post about my kid who plays soccer at a particular school," Dalva says. "If I'm the CFO at a private equity firm, the bad guys can send an email saying, 'Hi, my son is on the same soccer team. Thought you'd enjoy this photo of the boys.'" That's a terrific spear-phishing tactic, says Dalva. "I guarantee the recipient is going to open that attachment."

Hackers mine social media to determine who has access to critical data and who's connected to them. Martinez recalls one CFO who protected himself well from cyberthreats—until the hackers decided to target his daughter. "The daughter was on Facebook—they sent a spear-phishing email to her, and she unknowingly became infected with malware," says Martinez, who is also a senior adviser to the president and CEO of ACG Global and the Kogod Cybersecurity Governance Center at American University. Through the daughter, the hackers were able to infect the CFO's computer and obtain passwords to steal a considerable amount of money, he says.

To address social media concerns, some executives decide not to create profiles on LinkedIn or other networks. But that creates more problems than it solves, Martinez says. "If you do that, you don't own your identify in that space—and you give someone else the ability to create a version of you," he says. He's seen hackers create fake profiles of prominent executives and infect all the people who become connections.

Experts say the best defense against spear-phishing entails creating a culture of awareness, and that requires training. In December, Z Capital Partners conducted a mandatory training session on spam and email phishing. The firm also plans to send fake phishing emails to employees to gauge their awareness level and will follow up with additional training if needed, Pender says.

Ambrosini echoes the need for better user awareness, particularly since hackers have become more efficient. Phishing campaigns once required significant technical skill and could take weeks to set up correctly, he says. Today, thanks to easily accessible toolkits, hackers can create a phishing campaign in about 15 minutes. "The cost and time has gone down and the success rate has gone up," Ambrosini says. Years ago, hackers took a brute-force approach to break through firewalls—but now they realize there's no patch for human nature or human ignorance, he says. "There should be a lot more user education around these common hacking tactics and how to identify a malicious email," he adds. "User awareness may be the last line of defense between your company getting hacked or not."

EMBRACE THE BASICS

Sometimes firms create vulnerabilities by overlooking IT basics. Ambrosini recalls an "oh my gosh" moment for one client that seemed to have a robust security framework. "They had all the latest and greatest things, except they forgot to do one important thing—which was change the default credentials for the firewall," he says. Based on the login screen, Ambrosini's team could tell the client had a Cisco firewall. They obtained full access by using Cisco default credentials (in this case, "cisco" for the username and password). Hackers easily could have done the same. What's more, the client should have configured the firewall to be accessible internally. Instead, it was accessible from the Internet. That means anyone, anywhere could have attempted to log in, Ambrosini says, adding: "A lot of security risk comes down to basics."

"USER AWARENESS MAY BE THE LAST LINE OF DEFENSE BETWEEN YOUR COMPANY GETTING HACKED OR NOT."

Jim Ambrosini
Managing Director,
CohnReznick Advisory Group

"IF TODAY YOU'RE COMPROMISED, WHAT WILL YOU WISH YOU HAD DONE TO PROTECT YOUR VALUATION AND PROTECT YOURSELF FROM LIABILITY?"

Israel Martinez
President and CEO,
Axon Global, and Senior
Cybersecurity Adviser to
the President and CEO
of ACG Global

With the Federal Trade Commission and other regulators paying closer attention to cybersecurity policies, those basics have become even more vital. Says Martinez: "Look through the lens of, if today you're compromised, what will you wish you had done to protect your valuation and protect yourself from liability?" To that end, he recommends several actions that can help reduce risk:

- Begin implementing a simple version of the National Institute of Standards and Technology Cybersecurity Framework. "This framework has been accepted by the Department of Homeland Security, Fortune 500 companies and others," he says. "It's a good plan, but it's also a defensible plan from a liability standpoint."
- Adopt the five principles for enterprise cyberrisk management that the National Association of Corporate Directors recommends. "It is about creating awareness and accepting at a board level that cyber is an enterprise risk management issue more than a technology issue," Martinez says.
- Download the Sans Institute Top 20 CIS Critical Security Controls at Sans.org. "This is the recommended set of actions for cyberdefense that provides specific ways to stop today's most pervasive and dangerous attacks," he says.

"YOUR PREPARATION FOR DEALING WITH (AN INCIDENT) IS GOING TO AFFECT HOW BAD THE BREACH IS."

Dave Dalva
VP of Security Science,
Stroz Friedberg

HAVE A RESPONSE PLAN

Although a strong cybersecurity program is crucial, it's just as important to assume those efforts will fail—meaning, have an incident response plan in place. "Your preparation for dealing with (an incident) is going to affect how bad the breach is," Dalva says. That includes who needs to be involved in decision-making, who needs to be involved in notification and communication, when to bring in law enforcement, and how to communicate with limited partners.

When firms try to improvise a response after a breach, it can make the damage worse. "Communication may be inefficient, you might be saying the wrong things to the wrong people, and it's going to hurt you," he adds.

Dalva runs tabletop exercises with his clients by creating an attack simulation. "We follow the incident response plan, and we always learn things," he says. "The PE guys really appreciate the complexity of dealing with the aftermath." //

S.A. Swanson is a business writer based in the Chicago area who frequently writes about technology.